

# **AUDIT OF INFORMATION SECURITY PROGRAM**

*Department of Transportation*

*Report Number: FI-2009-003*

*Date Issued: October 8, 2008*



# Memorandum

U.S. Department of  
Transportation  
Office of the Secretary  
of Transportation  
Office of Inspector General

Subject: ACTION: Audit of Information Security  
Program, Department of Transportation,  
Report Number: FI-2009-003

Date: October 8, 2008

From: Calvin L. Scovel III  
Inspector General

Reply to  
Attn. of: JA-20

To: Chief Information Officer

This report presents the results of our annual audit of the Department of Transportation's (DOT) information security program and practices, as required by the Federal Information Security Management Act of 2002 (FISMA). FISMA further requires that our evaluation include testing of a representative subset of systems and an assessment, based on our testing, of the Department's compliance with FISMA and applicable requirements. On July 14, 2008, the Office of Management and Budget (OMB) issued M-08-21, *Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, which provides instructions for inspectors general to use in completing this year's FISMA evaluation, including the OMB template.

Consistent with FISMA and OMB requirements, our audit objective was to determine the effectiveness of DOT's information security program and practices. Specifically, we assessed the status of DOT's (1) implementation of minimum security standards, including progress in addressing issues identified previously in risk categorization and managing corrective actions; (2) configuration management, including deployment of baseline configurations and addressing telecommuting issues; (3) incident-handling and reporting; and (4) renewed initiatives in addressing Air Traffic Control system security weaknesses, including business continuity planning and testing of operational systems security outside of the computer laboratory.

As instructed, we tested a representative subset of the Department's systems, and included the results in OMB's required template (see Exhibit A and Table 7 in Exhibit B). Our testing included interviews with key information security personnel, reviews of technical documentation, and analysis of the Department's reported information security statistics. We conducted our audit in accordance with generally accepted government auditing standards. Those standards require

that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Details of our scope and methodology are described in Exhibit B.

## **INTRODUCTION**

FISMA requires Federal agencies to identify and provide security protection commensurate with the risk and magnitude of harm resulting from the loss of, misuse of, unauthorized access to, disclosure of, disruption to, or modification of information collected or maintained by or on behalf of an agency. FISMA and its predecessor, the Government Information Security Reform Act (GISRA), required the inspectors general to evaluate agencies' information security programs and practices.

The Department has 13 Operating Administrations that, for Fiscal Year (FY) 2008, reported a total of 425 information systems, of which 62 percent belong to the Federal Aviation Administration (FAA). Among the systems the Department maintains and operates is the air traffic control system, which the President has designated as part of the critical national infrastructure. Other systems owned by the Department include safety-sensitive surface transportation systems and financial systems that are used to manage and disburse over \$50 billion in Federal funds each year. In FY 2008, the departmental IT budget totaled about \$2.8 billion. Systems inventory counts for FY 2007 and FY 2008 for each Operating Administration are detailed in Exhibit C.

## **RESULTS IN BRIEF**

The Department's information security program and practices are not effective. As a result, the Department is not in compliance with FISMA and OMB requirements for security information systems and providing privacy protection of personally identifiable information (PII). Last year we reported that the overall effectiveness of DOT's information security program declined because management had to divert resources and attention to resolving Headquarters move-related issues.<sup>1</sup> While we observed some operational improvements, we nonetheless continued to see a decline in the Department's program and practices. (See the comparison between these 2 years in Exhibit D). As noted in Exhibit E, our prior year's information security-related recommendations have not been fully implemented.

---

<sup>1</sup> *DOT Information Security Program*, OIG Report FI-2008-001, October 10, 2007.

Developing a robust information security program, including implementation of our current and prior years' recommendations, requires (1) the Chief Information Officer (CIO) Office to effectively oversee Operating Administrations' implementation of departmental policies/guidance, and (2) stability in the Office of the Chief Information Security Officer (CISO). However, when compared with some of his counterparts in other Federal agencies and other appointed officials within the Department, the DOT CIO has limited influence on Operating Administrations. Unless there are management or budgeting consequences, Operating Administrations are likely to continue the practice of not effectively implementing departmental policies/guidance. We are making a recommendation to increase Operating Administrations' accountability. During FY 2008, the Department's performance was also hindered by significant turnover in the Office of the CISO.

For FY 2008, we found:

1. *The Department has not established adequate policies or procedures to implement and maintain an effective Departmentwide information security program or to address key OMB privacy requirements.* Specifically, the Department has a backlog of information-security policy awaiting publication and has not addressed key privacy requirements. For example, OMB mandated that—by September 22, 2007—agencies develop and implement a “breach-notification policy” and a plan to reduce the use of Social Security numbers. This has not happened at DOT. Without this policy, the Department cannot effectively direct or ensure that citizens whose private information is compromised are properly notified. We also found that the Department has not established a FISMA data collection cut-off date, as requested by OMB. Without a cut-off date, the Department does not have sufficient time to perform meaningful internal review or assess the results submitted to it by the Operating Administrations.
2. *The Department was not adequately protecting its computer networks.* Specifically, it was not effectively managing the configuration of the commercial software installed on departmental computers. Further, it has not fully developed sufficient security incident-monitoring and -reporting capabilities to protect the networks from intrusion. To reduce system vulnerabilities, both OMB and the Department require that commercial software, such as the Windows operating system and Oracle database system, be installed in accordance with specific Government security configuration standards. We have reported a lack of progress in this critical area since FY 2006. Last year, the Department reported that less than 50 percent of departmental computers were in compliance with configuration standards. This year, however, the Department was not able

to track Operating Administration compliance rates. Meanwhile, our testing continued to find computers without proper configuration, resulting in unnecessary vulnerabilities to departmental networks.

During FY 2008, the Department established a consolidated Cyber Security Management Center (CSMC) and a common framework for Departmentwide incident-monitoring and -reporting. This not only improved visibility of Headquarters networks for security monitoring, but also better positioned the Department to combat increasing cyber security threats. However, DOT's ability to respond to computer security incidents remained hindered by insufficient intrusion-detection of field networks and late reporting of incidents involving the potential compromise of PII.

3. *The Department was not ensuring that all of its employees and contractors receive the appropriate degree of computer-security training needed to prevent them from contributing to security weaknesses and breaches.* In particular, the Department was unable to effectively track contractors who needed security-awareness or other specialized security training. In addition, the Department did not address collaborative Web technologies in its security-awareness training, as required by OMB.
4. *The Department was not identifying all information-security weaknesses or ensuring the timely resolution and prioritization of those that are identified.* The Department is required to track and manage information security weaknesses in plans of actions and milestones (POA&M). We continued to find information-security weaknesses that were identified but not included in POA&Ms. Of the weaknesses that were identified and tracked in the Department's POA&M system, many of the high and moderate weaknesses were not remediated in a timely manner, resulting in unnecessary vulnerabilities in the Department's systems. For example, we found that remediation of unencrypted laptops containing PII was past due for more than a year. We also found many for which the priority level had not been assigned, and the cost of completing the remedial actions had not been estimated for more than half of the security weaknesses in the POA&M database. Without cost estimates and adequate prioritization, the Department cannot effectively and efficiently resolve information security weaknesses.
5. *The Department was not sufficiently protecting its systems or ensuring that they can be recovered when necessary.* The Department has not adequately identified all systems that provide services to citizens via the Internet and therefore are subject to OMB e-authentication requirements, and it is not validating that those requirements have been met for the

e-authentication systems it has identified. E-authentication provides assurance to each citizen that the Department is protecting private information by ensuring that only the citizen can access the account. In addition, we noted that 8 of 16 sampled systems did not have certifications and accreditations (C&A) that complied with National Institute of Standards and Technology (NIST) standards. Further, 20 of the Federal Highway Administration's (FHWA) 26 systems had not been recertified and were operating without accreditation, including two high-impact systems whose certifications and accreditations expired in November 2007. Finally, the Department is not adequately testing all of its system contingency plans and therefore cannot ensure that such plans will enable the recovery of essential systems in the event of disruption.

Last year, we reported that the Department needed to better secure network connections to allow employees to telecommute without creating additional vulnerabilities when connecting unsecure home computers to Department networks. According to management, the Department is currently using specialized software to check for basic security controls in employee home computers, such as firewalls and anti-virus software, before granting network connections. While this does mitigate some of the risks, these security checks are not sufficient because they do not determine whether employee home computers contain any malicious software that could compromise the Department's networks or systems. Consistent with our prior year's recommendation, we encourage departmental officials to continue exploring alternatives to support telecommuting initiatives while protecting departmental networks. Because these issues were previously reported, we are not including additional details in this report.<sup>2</sup>

During FY 2008, as part of its renewed initiatives in addressing air traffic control systems security—part of the Nation's critical infrastructure—FAA made progress in implementing a business continuity plan for air traffic control en route centers.<sup>3</sup> However, its ability to handle long-term service disruptions remains unknown because of unresolved operational issues. FAA has also expanded security evaluations of air traffic control systems outside of the computer laboratory. Yet FAA's methodology for evaluating systems security, including risk categorization, is not adequate to ensure that operational systems are properly protected. These concerns will be the subject of a separate report. Consequently, details related to these issues are not included in this report.

We are making a series of recommendations, beginning on page 19, to help the Department improve its information security and privacy programs. A draft of

---

<sup>2</sup> We reported our concerns with allowing telecommuting employees to connect with the Department's networks using home computers on page 17 of *DOT Information Security Program*, OIG Report FI-2008-001, October 10, 2007.

<sup>3</sup> En route centers are responsible for directing high-altitude traffic and disseminating flight information to all other air traffic control facilities.

this report was provided to the Department's CIO on September 30, 2008. On October 7, 2008, we received the CIO's response, which can be found in its entirety in the Appendix. The CIO concurred with our findings and recommendations and in 30 days will provide written comments describing the actions and milestones that will be taken to implement the recommendations.

## **FINDINGS**

### **Policies and Procedures Were Inadequate To Ensure Information Security and Privacy**

The Department had not developed adequate policies or procedures to establish and maintain an effective Departmentwide information security program or to address key OMB privacy requirements. We believe the absence of comprehensive policies and procedures is contributing to the continuing decline in the effectiveness of the Department's information security program and practices. Further, the Department's lack of a cut-off date for its FISMA reporting has inhibited its ability to oversee its information security program.

#### *Large Backlog of Information Security Policies Awaited Publication*

FISMA requires the Department to develop an information security program that includes policies and procedures that are based on the risk assessments to cost-effectively reduce information security risks to an acceptable level and to ensure that information security is addressed throughout the life cycle of each agency information system. The Department's CIO Office had a large backlog of draft information technology security policy in development. The Department identified 52 topics that require IT security policy. To date, it has issued policy on only 11 (21 percent). The other 41 topics remain unaddressed or have policy under development or in draft form (see Table 1). A few examples of key policies that are unaddressed or otherwise not final include policies that address configuration management, risk-level categorization, backup and contingency planning, intrusion detection, access control, passwords, wireless networking, remote access, risk assessment, and security planning.

**Table 1. Status of DOT Information Security Policies**

<b>Policy Status</b>	<b>Number</b>
Final	11
Draft	14
Under Development	19
Unaddressed	8
<b>Total</b>	<b>52</b>

Source: OIG analysis

Without adequate and comprehensive information technology security policies, the Department cannot establish or maintain an effective information security program, which includes (1) providing direction to the Operating Administrations, its employees, or its contractors on information security; (2) enforcing compliance with key information security requirements; and (3) ensuring that security risks are reduced in a cost-effective and consistent manner. We further believe that the absence of key policies is contributing to the Department's weaknesses in securing its networks, protecting its systems, providing security training, and resolving other information technology issues. These matters are further described below.

#### ***Key Privacy Requirements Have Not Been Addressed***

OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, required agencies to (1) develop and implement a "breach notification policy" by September 22, 2007; (2) review current holdings of all personally identifiable information and ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete, and reduce them to the minimum necessary for the proper performance of a documented agency function; (3) develop a plan by September 22, 2007, to reduce the use of Social Security numbers by November 22, 2009; and (4) implement a "rules and consequences policy" outlining the rules of behavior and identifying consequences and corrective actions available for failure to follow these rules.

The breach notification policy is still in draft form and, according to the DOT Privacy Officer, is still undergoing revision. This policy is now over a year overdue. In addition, the Department has still not developed a "rules and consequences" policy. According to our most recent privacy report,<sup>4</sup> the agency has not completed its reviews to determine if all systems containing PII have been

---

<sup>4</sup> *Review of DOT Privacy Policies and Procedures*, OIG Report Number FI-2008-077, September 9, 2008.



identified. Specifically, the Privacy Office could not provide assurance that 320 systems do not contain PII.

The Department's plan to reduce Social Security numbers likewise remains in draft form and is also over a year late. This plan, which is part of the Department's M-07-16 DRAFT Action Plan, is extremely high level and is missing goals, specific tasks, interim milestones, and assignment of responsibilities. In addition, the plan has not been implemented and it is increasingly unlikely that the Department will meet OMB's November 22, 2009, deadline for completing the reduction of the use of Social Security numbers. The following table encompasses the Department's entire draft plan to eliminate unnecessary use of Social Security numbers:

**Table 2. DOT Draft Plan to Eliminate Unnecessary Use of Social Security Numbers**

Tasks	Actions
<p><b>Review and eliminate unnecessary use of SSNs</b></p> <p><b>Develop plan, within 18 months, to eliminate unnecessary collection and use of SSNs</b></p> <p><b>Explore alternatives to use of SSNs as a personal identifier</b></p>	<ul style="list-style-type: none"> <li>• <b>Arrange meeting with HR, Security, OGC (Stand-up SSN Elimination Task Force).</b></li> <li>• Initial review performed for OMB in Dec 2006.</li> <li>• Draft/send email to OA Privacy Officers about need to update this review and ask for their plans to do so.</li> <li>• Collect and analyze responses from the PII System Owner Survey.</li> <li>• Draft DOT wide plan for submission to OMB.</li> <li>• Participate in Governmentwide efforts to explore alternatives.</li> </ul>

Source: DOT

Without implementing these key privacy requirements, the Department cannot (1) ensure that all PII is properly identified and protected, (2) minimize the risk that Social Security numbers will be exposed to parties who do not have a legitimate need to know or possess them, (3) ensure that affected citizens are adequately notified in a timely manner when affected by breaches of personally identifiable or other sensitive information, or (4) implement consequences for employees who willfully or otherwise break privacy rules. Consequently, the Department may unwillingly contribute to problems with identity theft, law enforcement, or even national security.

### *FISMA Data-Collection Cut-Off Date Has Not Been Established*

In M-08-21, *Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, OMB requests that agencies set an internal cut-off date for FISMA data collection and report preparation. This cut-off date should permit adequate time for meaningful internal review and comment and resolution of any disputes before finalizing the agency's report to OMB. We found, however, that DOT's Office of the CIO (OCIO) has not set a Departmentwide FISMA cut-off date. Instead, the OCIO allows updates to the information to occur right up to the FISMA deadline. (*Note: OIG used a cut-off date of August 31, 2008, to allow for the timely completion of its audit on DOT's information security program and practices.*)

Without an adequate internal Departmentwide cut-off date, the Department does not have sufficient time to perform meaningful internal review or assess the results submitted to it by the Operating Administrations. Because OIG uses a cut-off date and the Department does not, there will be timing differences between OIG's and the OCIO's respective FISMA reports. In addition, some information may not be provided to OIG in a timely manner for inclusion in its report. Further, this results in limited time for the Department and OIG to resolve disputes or differences in their respective reports, and for the Department to develop a timely corrective action plan that OIG can review prior to issuing its FISMA audit report.

### **DOT Networks Were Not Adequately Protected From Intrusion**

Last year we reported that deficiencies were evident in network computers' configurations, and that reporting of security incidents was incomplete and inaccurate. For FY 2008, the Department did not effectively manage baseline system configurations or track compliance with configuration standards, did not sufficiently deploy Federal Desktop Core Configuration (FDCC) requirements, and deployed software that was not properly configured. In addition, the Department's capability to respond to computer security incidents is hindered due

to the low visibility of field networks and untimely reporting of certain incidents pertaining to PII.

### *Baseline Configuration Standards Have Not Been Fully Implemented*

To reduce the risk of hostile attacks based on known vulnerabilities in commercial off-the-shelf software, such as the Windows Operating and Oracle Database systems, agencies are required to configure such commercial software in accordance with NIST or agency security standards. Last year, DOT centrally tracked Operating Administrations' implementation of departmental baseline configuration standards, which enabled DOT to report that 29 percent of its systems conformed to these standards. However, this year DOT had no such tracking capability, and was not able to share Operating Administrations' compliance status with OIG. According to OCIO officials, DOT began the transition to the Cyber Security Assessment and Management tool (CSAM) as its authoritative FISMA reporting system during FY 2008. It also asked Operating Administrations to input their compliance status into CSAM. However, the required information was missing from CSAM. In addition, last year we reported that DOT issued a draft policy on configuration management. This policy was still marked as "under development" in September 2008.

OMB M-07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, required agencies that have deployed the Windows XP Operating System to adopt the security configurations developed by NIST. We randomly tested 33 Windows XP workstations located at DOT Headquarters, including one within OIG, and found none to be in full compliance with FDCC settings. The average compliance rate of these computers was less than 70 percent. The OCIO could not provide us with any documentation or justification of the deviations from the mandated configuration settings.

Without Departmentwide policy, tracking capability of implementation status of baseline configuration standards, and full deployment of FDCC security settings, the Department has no assurance that its computer systems have been adequately configured to minimize vulnerability. Indeed, during our review of one DOT system, we found that computers supporting the system were vulnerable to potential cyber attack due to inadequate configuration. This could obviously threaten DOT's business operations.

### *Critical Networks Lacked Comprehensive Intrusion-Detection Coverage*

FISMA requires agencies to have procedures for detecting, reporting, and responding to security incidents. Starting in FY 2008, two DOT incident-response centers were merged into the CSMC. Currently, CSMC is responsible for

providing intrusion-detection system (IDS) monitoring services<sup>5</sup> to all Operating Administrations. This helps the Department address increasing cyber security threats. CSMC has also improved monitoring coverage to DOT's Headquarters operations. However, it has limited IDS monitoring coverage for DOT's field operations. For example, other than the Volpe National Transportation Systems Center and FAA's regional offices, none of DOT's field operations were subject to CSMC monitoring.

According to the CSMC officials, effective IDS deployment to DOT's network requires close cooperation between CSMC and the Operating Administrations. Currently, this cooperation is lacking. In fact, DOT management has not fully mapped its network infrastructure, including the locations of critical network points, resulting in deployment of IDS sensors on an ad-hoc basis, which has made CSMC monitoring of DOT networks less effective. Without effectively deploying IDS monitoring capability, DOT cannot be fully aware of potential cyber attacks on its networks and, as a result, cannot take timely action to stop or further prevent these attacks.

### *PII Incidents Were Not Immediately Reported*

DOT policy, *Reporting Cyber Security Incidents and Sensitive Personally Identifiable Information (SPII) Exposures*, requires all cyber security incidents and SPII exposures be reported to CSMC immediately upon discovery. In addition, OMB M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, requires agencies to report all incidents involving PII to the United States Computer Emergency Readiness Team (US-CERT) within 1 hour of discovery. However, the Operating Administrations have not followed the departmental policy to report PII incidents internally to CSMC in a timely manner, which, in turn, prevented the incidents from being reported to US-CERT within OMB's required time frame.

We reviewed 38 PII-related cyber security incidents reported to CSMC between October 1, 2007 and July 31, 2008. Of these, ten (26 percent) were delayed in reporting to CSMC from 1 to 12 days. Further, CSMC did not report four PII incidents to US-CERT—including one that contained the dates of birth of 168 individuals. According to CSMC, dates of birth were not considered sensitive PII under departmental policy. Consequently, CSMC did not report this incident to US-CERT, which is in conflict with OMB's requirement to report all PII incidents within 1 hour.

---

<sup>5</sup> To effectively monitor and detect potential cyber security incidents on a network, sensors are installed at the various critical network points. These sensors automatically generate security alerts when potential cyber attacks are detected, and are usually monitored from a central location that responds to incidents, including intrusions.

### *Response to Detected Incidents Was Slow*

NIST Special Publication 800-61, *Computer Security Incident Handling Guide*, states that an incident-response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. We found, however, that Operating Administrations did not review and correct incidents referred by CSMC in a timely manner. For example, as of June 30, 2008, there were 233 unresolved incidents that needed remediation, 77 of which (33 percent) had been open for more than 3 months, including critical incidents like potentially unauthorized access to DOT computers.

Why did this occur? Because DOT did not have specific guidance or procedures in place to direct security officials on how to effectively remediate identified incidents. In addition, the lack of needed information, such as critical logging data and complete IP address information, impeded DOT's effort to accurately pinpoint the computers affected by incidents in order to take timely action.<sup>6</sup> Without timely and effective remediation of cyber incidents, the Department remains at risk for similar network compromises.

### **The Department Was Not Ensuring Adequate Security Training of Its Employees and Contractors**

FISMA requires the Secretary to ensure that the Department has sufficiently trained personnel to assist the agency in complying with FISMA and related policies, procedures, standards, and guidelines. FISMA also states that the required agencywide information security program shall include security-awareness training to inform personnel, including contractors, of information-security risks associated with their activities, and their responsibilities in complying with agency policies and procedures designed to reduce these risks. However, the Department had no mechanism with which to track contractors requiring security-awareness training. Also lacking was a policy for the use of collaborative Web technologies;<sup>7</sup> such technologies were likewise not included in DOT's security-awareness training, as is required by OMB.

FISMA further requires that the Secretary delegate to the CIO the authority to ensure compliance with the requirements imposed on the agency, including training personnel with significant responsibilities for information security. To

---

<sup>6</sup> An IP address is a unique numerical identification that is assigned to a computer on a network.

<sup>7</sup> Collaborative software is designed to help people involved in a common task achieve their goals and is the basis for computer-supported cooperative work. Examples of collaborative software include electronic calendars used to schedule events and automatically notify and remind group members about meetings; project management systems used to schedule, track, and chart steps in a project as it is being completed; and online spreadsheets used to share structured data and information.

date, the Department has been unable to provide us with any information on employees or contractors with significant information-security responsibilities who require or have taken specialized security training. Without such tracking capabilities, the Department cannot ensure that employees and contractors are receiving sufficient and appropriate security training.

Employees who are not properly trained about computer security may cause, contribute to, or become victims of the following vulnerabilities or security breaches: e-mail exploits, account or password sharing, inadequate safeguarding of passwords or computer resources, Internet misuse, corporate espionage, or social engineering. In addition, without including collaborative Web technologies in its security-awareness training, employees and contractors could misapply these technologies and enable access and review of sensitive DOT data and information by unauthorized personnel or entities. This could put sensitive or critical information at risk for unauthorized disclosure or use that could be detrimental to DOT and the general public.

### **Correction of Information Security Weaknesses Was Not Adequately Managed**

For FY 2008, the Department did not improve its management of information security weaknesses. DOT is required to track and manage information security weaknesses in POA&Ms; the Department uses CSAM to track its POA&Ms. For each weakness, these POA&Ms should identify a priority level, a cost estimate to complete the action, and a milestone date to indicate by when the action will be remediated. This information is critical if management is to prioritize, fund, and resolve information-security weaknesses in a timely manner. Last year, we reported that insufficient action had been taken to correct identified security deficiencies. We specifically noted that 30 percent of corrections (901 out of about 3000) were overdue for more than 6 months, and cost estimates to fix 60 percent of the deficiencies were missing.

We found information security weaknesses that were identified but not incorporated in POA&Ms. Of those that were identified and tracked in the POA&M system, there were many for which the priority level has not been assigned or the cost of completing the remedial actions has not been estimated. In addition, many of the high and moderate weaknesses were not remediated in a timely manner.

- *Weaknesses Not Recorded.* OMB M-08-21 requires that POA&Ms include all security weaknesses found during any review done by, for, or on behalf of the agency, including Government Accountability Office audits, financial system audits, and critical infrastructure vulnerability

assessments. In addition, the memorandum requires that these plans be the authoritative agencywide management tool, inclusive of all evaluations. However, in our review of the 16 sampled IT systems, we found that 8 (ARTS IIIA, ACE-IDS, OASIS, ADAS, CSAM, HMPIP, FHWA Network, and TransStats) did not report all known IT security weaknesses in POA&Ms.

- *Weaknesses Not Prioritized or Lacking Cost Estimates.* OMB M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, states that POA&Ms should detail resources required to accomplish the elements of the plan and be used to prioritize corrective actions. Of the 4,286 open information security weaknesses, 939 (22 percent) were not prioritized as high, moderate, or low; and 2,493 (58 percent) did not indicate the cost to resolve/remediate them (see Table 3).

**Table 3. IT Security Weaknesses Lacking Categorization and/or Cost Data**

OA	Total IT Security Weaknesses	Weaknesses Not Categorized as High, Moderate, or Low	Estimated Cost Not Identified
FAA	3,049	710	1,703
FHWA	269	5	266
FMCSA	28	2	25
FRA	257	200	2
FTA	17	15	1
MARAD	337	5	191
NHTSA	7	0	7
OIG	15	0	6
OST	53	2	38
PHMSA	128	0	128
RITA	59	0	59
SLSDC	0	0	0
STB	67	0	67
<b>Total</b>	<b>4,286</b>	<b>939</b>	<b>2,493</b>
<b>Percentage</b>		<b>22%</b>	<b>58%</b>

Source: DOT

- *Weaknesses Overdue for Correction.* We also found 986 information security weaknesses whose corrective actions were either overdue or did not have a scheduled completion date (see Table 4).

**Table 4. IT Security Weaknesses Overdue for Mitigation**

OA	Total IT Security Weaknesses	Total Overdue or Without Scheduled Completion Date	OVERDUE					No Scheduled Completion Date
			1-60 days	61-90 days	91-120 days	121 days-1 year	>1 year	
STB	67	67	0	0	0	0	52	15
SLSDC	0	0	0	0	0	0	0	0
RITA	59	59	0	0	1	6	18	34
PHMSA	128	128	0	49	0	24	27	28
OST	53	36	0	1	14	3	17	1
OIG	15	9	0	0	0	8	1	0
NHTSA	7	6	0	0	0	0	4	2
MARAD	337	5	1	1	1	0	0	2
FTA	17	0	0	0	0	0	0	0
FRA	257	181	2	0	30	0	6	143
FMCSA	28	9	0	3	0	0	6	0
FAA	3,049	217	7	5	4	2	7	192
FHWA	269	269	0	0	2	31	226	10
<b>Total</b>	<b>4,286</b>	<b>986</b>	<b>10</b>	<b>59</b>	<b>52</b>	<b>74</b>	<b>364</b>	<b>427</b>
<b>Percentage</b>		<b>23%</b>	<b>0.2%</b>	<b>1.4%</b>	<b>1.2%</b>	<b>1.7%</b>	<b>8.5%</b>	<b>10%</b>

Source: DOT

Without a compliant POA&M process, the Department cannot ensure that its systems are adequately secured and protected. Specifically, without cost estimates, proper risk categorizations, or milestones to resolve or mitigate all weaknesses, it is difficult or impossible for the Department to adequately prioritize and resolve open weaknesses. As a result, weaknesses of lesser urgency may get resolved before critical ones. In addition, allowing weaknesses to remain unaccounted for, unresolved, or unmitigated for extended periods of time allows for unnecessary vulnerabilities and exposures that may be exploited by intruders, or may otherwise compromise the availability or integrity of essential systems and data.



## **DOT Systems Were Not Sufficiently Protected or Adequately Tested To Ensure Recovery**

The Department was not sufficiently protecting its systems or ensuring that they can be recovered when necessary. Last year we reported that 11 (52 percent) of 21 sampled systems did not meet minimum security-protection requirements. For FY 2008, there were no significant improvements.

### *Mandated Online Authentication Requirements Were Not Being Met*

The Federal Government wants its citizens to be able to access Government services quickly and easily through the Internet. To ensure that online Government services are secure and protect privacy, some type of identity verification or authentication (referred to as *e-authentication*) is needed. OMB M-04-04, *E-Authentication Guidance for Federal Agencies*, prescribes a process for agencies to use in determining what level of assurance is needed to verify the identity of the requester. This process includes, but is not limited to, conducting a risk assessment of the e-government system, validating that the implemented system has achieved the required assurance level, and periodically reassessing the system to determine technology-refresh requirements.

Our review of the OCIO's inventory of e-authentication systems and supporting documentation for three sample systems managed by the Federal Motor Carrier Safety Administration (FMCSA) and the Federal Railroad Administration (FRA), including certification and accreditation packages, found the following:

- No e-authentication documentation was available to support the three sampled DOT system classifications and categorized assurance levels.
- The risk assessments of the three systems did not contain any information regarding e-authentication.
- The system security plans of the three systems did not address e-authentication requirements.
- FMCSA and FRA officials were unaware whether any validation of the three systems had occurred, and could not provide any documentation to support validation.

In addition, the Department has not identified all systems requiring e-authentication. For example, FAA's Medical Support System, which allows thousands of airmen to complete medical applications online through the Internet, was not included in the inventory of systems that requires e-authentication.

Without supporting e-authentication documentation and a complete inventory of e-authentication systems, the Department has no assurance that its IT systems requiring e-authentication are adequately identified and protected. Further, without considering e-authentication requirements during the certification and accreditation process, changes to e-authentication levels or other matters may occur without an appropriate reassessment of each system's e-authentication requirements.

### *Systems Were Not Certified and Accredited in Accordance with NIST Standards*

NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, states that the security accreditation package documents the results of the security certification and provides the authorizing official with the essential information needed to make a credible, risk-based decision on whether to authorize operation of the information system. It further states that the security accreditation package should contain an approved system security plan, a security assessment report, and a POA&M. Half (8) of our 16 sampled systems did not meet these core requirements (see Table 5).

**Table 5: Sampled Systems' C&A Results**

<b>OA</b>	<b>Sampled Systems</b>	<b>Systems Without Fully Compliant C&amp;As</b>
<b>FAA</b>	11	5
<b>FHWA</b>	1	1
<b>FMCSA</b>	1	1
<b>FRA</b>	1	0
<b>OST</b>	1	0
<b>RITA</b>	1	1
<b>Total</b>	<b>16</b>	<b>8</b>

Source: OIG

OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, requires that systems be reauthorized (i.e., accredited) at least once every 3 years. However, 20 of FHWA's 26 systems had not been recertified, and were operating without accreditation, including two high-impact systems whose certifications and accreditations expired in November 2007. Without proper certification and accreditation, the Department lacks a crucial management control that ensures that systems are properly assessed for risk, have been independently tested, and have identified and sufficiently mitigated weaknesses. Consequently,

management cannot ensure that systems are operating without unacceptable risks or weaknesses.

### *Contingency Plans Were Not Being Tested*

OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, requires agencies to establish and periodically test the capability to continue providing service within a system based upon the needs and priorities of the participants of the system. NIST Special Publication 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, further requires that agencies test and update their system contingency plans at least annually. As shown in table 6, only 11 of 16 sampled systems had a contingency plan. In addition, only 9 of the 11 contingency plans had complied with testing requirements.

**Table 6: Sampled Systems' Contingency Status**

OA	Sampled Systems	Systems With Contingency Plans	Systems With Tested Contingency Plans
FAA	11	7	6 <sup>a</sup>
FHWA	1	1	1
FMCSA	1	1	1
FRA	1	1	1
OST	1	1	0
RITA	1	0	--
<b>Total</b>	<b>16</b>	<b>11</b>	<b>9</b>

<sup>a</sup>Includes a system for which testing was not yet due.

Source: OIG

Without adequate preparation and testing of system contingency plans, DOT cannot ensure that systems will operate properly or in a timely manner during an emergency or service disruption. Loss of DOT IT systems would limit DOT management's ability to perform its missions, including its critical functions in serving the public.

## **RECOMMENDATIONS**

In order to reduce the vulnerabilities currently inherent in the Department's information security program, we recommend that the Chief Information Officer do the following:

### **Information Security and Privacy Programs:**

1. Provide information security performance metrics to be included in Operating Administration CIOs' performance standards and subsequently provide input on their performance in addressing these metrics;
2. Develop and issue comprehensive, compliant information-security policies and procedures as required by FISMA, OMB, and NIST;
3. Complete review of its draft breach-notification policy, perform revisions as necessary to conform to OMB requirements, and issue an official breach-notification policy;
4. Review and finalize its plan to reduce Social Security numbers, and implement the reduction of Social Security numbers in the time frame set forth by OMB.
5. Issue a policy outlining the rules of behavior and identifying consequences and corrective actions available for failure to protect privacy;
6. Establish a departmentwide internal FISMA cut-off date that allows sufficient time for the Department to conduct meaningful internal review, which includes evaluating the accuracy of the data it includes in its FISMA report as well as time to resolve any potential disputes with the OIG;
7. Maintain an adequate audit trail of data supporting FISMA reports as of the selected cut-off date;

### **Network Security:**

8. Assign a priority to finalizing the DOT configuration management policy;
9. Require Operating Administrations to periodically report status of baseline configuration compliance and independently validate compliance status reported by Operating Administrations;

10. Implement NIST FDCC settings on the Windows XP workstations on the DOT Common Operating Environment, require Operating Administrations to implement FDCC settings on Operating Administrations' Windows XP workstations, and document any required deviations from those settings;
11. Establish a timetable for Operating Administrations to work with CSMC to deploy monitoring devices covering all DOT critical networks;
12. Enforce Operating Administrations' reporting of PII-related security incidents to CSMC immediately upon discovery, as specified in DOT policy;
13. Revise DOT policies to meet the OMB requirement for reporting PII incidents;
14. Implement procedures for Operating Administrations to take timely remedial action for identified incidents;
15. Direct CSMC and Operating Administrations to work together to collect and share the information needed for cyber incident-response reporting, such as IP- address assignment and critical logging data;

**Security Training:**

16. Enforce the requirements for all employees and contractors to take security-awareness training in order to gain and maintain access to Department systems;
17. Establish a tracking system or other process that effectively and routinely accounts for all active contractors requiring security training;
18. Establish a mechanism to identify and train employees and contractors requiring specialized security training;
19. Include collaborative Web technologies in the Department's required security-awareness training;

**Management of Information Security Weaknesses:**

20. Ensure that all weaknesses that are identified during reviews, including certification and accreditation, and that require remediation, are tracked in the Department's POA&M system;
21. Establish adequate policies for timeliness of remediation and enforce such policies;

22. Require that all identified weaknesses include a cost estimate and that these estimates, along with the severity of the weakness, be used to prioritize these weaknesses for correction;

**Systems Security:**

23. Implement a process to ensure that all departmental systems that require e-authentication are identified in the e-authentication system inventory and that the necessary e-authentication supporting documentation is obtained or developed for these systems;
24. Ensure that all systems that require e-authentication have certification and accreditation packages that include support for e-authentication in the appropriate sections of their system security plans and risk assessments;
25. Validate that e-authentication systems have operationally achieved the required assurance level;
26. Require development and appropriate annual testing of system contingency plans and ensure that tested contingency plans are updated based on the results of the contingency plan tests performed; and
27. Enforce certification and accreditation requirements uniformly throughout the Department.

**MANAGEMENT COMMENTS AND OFFICE OF INSPECTOR  
GENERAL RESPONSE**

A draft of this report was provided to the Department's CIO on September 30, 2008. On October 7, 2008, we received the Department CIO's response, which can be found in its entirety in the Appendix. The CIO concurred with our findings and recommendations and will provide, in 30 days, written comments describing the specific actions and milestones that will be taken to implement the recommendations.

## **ACTIONS REQUIRED**

We will review the Chief Information Officer's detailed action plans to determine whether they satisfy the intent of our recommendations. All corrections are subject to follow-up provisions in DOT Order 8000.1.C. We appreciate the courtesies and cooperation of the CIO Office and the Operating Administrations' representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-1959; David Dobbs, Principal Assistant Inspector General for Auditing and Evaluation, at (202) 366-0500; or Rebecca C. Leng, Assistant Inspector General for Financial and Information Technology Audits, at (202) 366-1407.

#

cc: Deputy Secretary  
Assistant Secretary for Budget and Programs/Chief Financial Officer  
Acting Federal Aviation Administrator  
CIO Council Members  
Martin Gertel, M-1

Section C - Inspector General: Questions 1 and 2													
Agency Name:		Department of Transportation						Submission date:		October 1, 2008			
Question 1: FISMA Systems Inventory													
1. As required in FISMA, the IG shall evaluate a representative subset of systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.													
In the table below, identify the number of agency and contractor information systems, and the number reviewed, by component/bureau and FIPS 199 system impact level (high, moderate, low, or not categorized). Extend the worksheet onto subsequent pages if necessary to include all Component/Bureaus.													
Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor of an agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.													
Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.													
Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing													
2. For the Total Number of Systems reviewed by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.													
Bureau Name	FIPS 199 System Impact Level	Question 1						Question 2					
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems (Agency and Contractor systems)		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and reviewed in the past year		c. Number of systems for which contingency plans have been tested in accordance with policy	
		Number	Number Reviewed	Number	Number Reviewed	Total Number	Total Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
Federal Aviation Administration	High	18	3	0		18	3	1	33%	2	67%	0	0%
	Moderate	157	6	12		169	6	5	83%	5	83%	5	83%
	Low	72	2	3		75	2	0	0%	2	100%	1	50%
	Not Categorized	2	0	0		2	0						
	<b>Sub-total</b>	<b>249</b>	<b>11</b>	<b>15</b>	<b>0</b>	<b>264</b>	<b>11</b>	<b>6</b>	<b>55%</b>	<b>9</b>	<b>82%</b>	<b>6</b>	<b>55%</b>
Federal Highway Administration	High	6	1			6	1	0	0%	0	0%	1	100%
	Moderate	13		1		14	0						
	Low	6				6	0						
	Not Categorized					0	0						
	<b>Sub-total</b>	<b>25</b>	<b>1</b>	<b>1</b>	<b>0</b>	<b>26</b>	<b>1</b>	<b>0</b>	<b>0%</b>	<b>0</b>	<b>0%</b>	<b>1</b>	<b>100%</b>
Federal Motor Carrier Safety Administration	High					0	0						
	Moderate	19	1	2		21	1	0	0%	1	100%	1	100%
	Low	1		1		2	0						
	Not Categorized					0	0						
	<b>Sub-total</b>	<b>20</b>	<b>1</b>	<b>3</b>	<b>0</b>	<b>23</b>	<b>1</b>	<b>0</b>	<b>0%</b>	<b>1</b>	<b>100%</b>	<b>1</b>	<b>100%</b>
Federal Railroad Administration	High					0	0						
	Moderate	11		3	1	14	1	1	100%	1	100%	1	100%
	Low	4		3		7	0						
	Not Categorized					0	0						
	<b>Sub-total</b>	<b>15</b>	<b>0</b>	<b>6</b>	<b>1</b>	<b>21</b>	<b>1</b>	<b>1</b>	<b>100%</b>	<b>1</b>	<b>100%</b>	<b>1</b>	<b>100%</b>
Federal Transit Administration	High					0	0						
	Moderate	4				4	0						
	Low	1				1	0						
	Not Categorized					0	0						
	<b>Sub-total</b>	<b>5</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>5</b>	<b>0</b>	<b>0</b>		<b>0</b>		<b>0</b>	
Maritime Administration	High	1				1	0						
	Moderate	8				8	0						
	Low	4				4	0						
	Not Categorized					0	0						
	<b>Sub-total</b>	<b>13</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>13</b>	<b>0</b>	<b>0</b>		<b>0</b>		<b>0</b>	
National Highway Traffic Safety Administration	High					0	0						
	Moderate	6		2		8	0						
	Low	2		1		3	0						
	Not Categorized					0	0						
	<b>Sub-total</b>	<b>8</b>	<b>0</b>	<b>3</b>	<b>0</b>	<b>11</b>	<b>0</b>	<b>0</b>		<b>0</b>		<b>0</b>	
Office of the Inspector General	High					0	0						
	Moderate	2				2	0						
	Low					0	0						
	Not Categorized					0	0						
	<b>Sub-total</b>	<b>2</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>2</b>	<b>0</b>	<b>0</b>		<b>0</b>		<b>0</b>	
Office of the Secretary	High			3	1	3	1	1	100%	1	100%	0	0%
	Moderate	19		7		26	0						
	Low	6		8		14	0						
	Not Categorized	1				1	0						
	<b>Sub-total</b>	<b>26</b>	<b>0</b>	<b>18</b>	<b>1</b>	<b>44</b>	<b>1</b>	<b>1</b>	<b>100%</b>	<b>1</b>	<b>100%</b>	<b>0</b>	<b>0%</b>
Pipeline and Hazardous Materials Safety Administration	High					0	0						
	Moderate			2		2	0						
	Low	1		1		2	0						
	Not Categorized					0	0						
	<b>Sub-total</b>	<b>1</b>	<b>0</b>	<b>3</b>	<b>0</b>	<b>4</b>	<b>0</b>	<b>0</b>		<b>0</b>		<b>0</b>	
Research and Innovative Technology Administration	High	1	1			1	1	0	0%	1	100%	0	0%
	Moderate	5		3		8	0						
	Low					0	0						
	Not Categorized					0	0						
	<b>Sub-total</b>	<b>6</b>	<b>1</b>	<b>3</b>	<b>0</b>	<b>9</b>	<b>1</b>	<b>0</b>	<b>0%</b>	<b>1</b>	<b>100%</b>	<b>0</b>	<b>0%</b>
Saint Lawrence Seaway Development Corporation	High					0	0						
	Moderate					0	0						
	Low	1				1	0						
	Not Categorized					0	0						
	<b>Sub-total</b>	<b>1</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>1</b>	<b>0</b>	<b>0</b>		<b>0</b>		<b>0</b>	
Surface Transportation Board	High					0	0						
	Moderate	2				2	0						
	Low					0	0						
	Not Categorized					0	0						
	<b>Sub-total</b>	<b>2</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>2</b>	<b>0</b>	<b>0</b>		<b>0</b>		<b>0</b>	
<b>Agency Totals</b>	<b>High</b>	<b>26</b>	<b>5</b>	<b>3</b>	<b>1</b>	<b>29</b>	<b>6</b>	<b>2</b>	<b>33%</b>	<b>4</b>	<b>67%</b>	<b>1</b>	<b>17%</b>
	<b>Moderate</b>	<b>246</b>	<b>7</b>	<b>32</b>	<b>1</b>	<b>278</b>	<b>8</b>	<b>6</b>	<b>75%</b>	<b>7</b>	<b>88%</b>	<b>7</b>	<b>88%</b>
	<b>Low</b>	<b>98</b>	<b>2</b>	<b>17</b>	<b>0</b>	<b>115</b>	<b>2</b>	<b>0</b>	<b>0%</b>	<b>2</b>	<b>100%</b>	<b>1</b>	<b>50%</b>
	<b>Not Categorized</b>	<b>3</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>3</b>	<b>0</b>	<b>0</b>		<b>0</b>		<b>0</b>	
	<b>Total</b>	<b>373</b>	<b>14</b>	<b>52</b>	<b>2</b>	<b>425</b>	<b>16</b>	<b>8</b>	<b>50%</b>	<b>13</b>	<b>81%</b>	<b>9</b>	<b>56%</b>



Section C - Inspector General: Question 3			
Agency Name: Department of Transportation			
Question 3: Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory			
3.a.	<p>The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.</p> <p>Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.</p> <p>Response Categories:</p> <ul style="list-style-type: none"> <li>- Rarely- for example, approximately 0-50% of the time</li> <li>- Sometimes- for example, approximately 51-70% of the time</li> <li>- Frequently- for example, approximately 71-80% of the time</li> <li>- Mostly- for example, approximately 81-95% of the time</li> <li>- Almost Always- for example, approximately 96-100% of the time</li> </ul>	Rarely (0-50% of the time)	
3.b.	<p>The agency has developed a complete inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.</p> <p>Response Categories:</p> <ul style="list-style-type: none"> <li>- The inventory is approximately 0-50% complete</li> <li>- The inventory is approximately 51-70% complete</li> <li>- The inventory is approximately 71-80% complete</li> <li>- The inventory is approximately 81-95% complete</li> <li>- The inventory is approximately 96-100% complete</li> </ul>	Inventory is 96-100% complete	
3.c.	The IG generally agrees with the CIO on the number of agency-owned systems. Yes or No.	Yes	
3.d.	The IG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency. Yes or No.	Yes	
3.e.	The agency inventory is maintained and updated at least annually. Yes or No.	Yes	
3.f.	If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please identify the known missing systems by Component/Bureau, the Unique Project Identifier (UPI) associated with the system as presented in your FY2008 Exhibit 53 (if known), and indicate if the system is an agency or contractor system.		
	Component/Bureau	System Name	Exhibit 53 Unique Project Identifier (UPI) {must be 23-digits}
	Number of known systems missing from inventory:		

Section C - Inspector General: Questions 4 and 5																		
<b>Agency Name:</b> Department of Transportation																		
<b>Question 4: Evaluation of Agency Plan of Action and Milestones (POA&amp;M) Process</b>																		
<p>Assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestones (POA&amp;M) process. Evaluate the degree to which each statement reflects the status in your agency by choosing from the responses provided. If appropriate or necessary, include comments in the area provided.</p> <p>For each statement in items 4.a. through 4.f., select the response category that best reflects the agency's status.</p> <p><b>Response Categories:</b></p> <ul style="list-style-type: none"> <li>- Rarely- for example, approximately 0-50% of the time</li> <li>- Sometimes- for example, approximately 51-70% of the time</li> <li>- Frequently- for example, approximately 71-80% of the time</li> <li>- Mostly- for example, approximately 81-95% of the time</li> <li>- Almost Always- for example, approximately 96-100% of the time</li> </ul>																		
4.a.	The POA&M is an agency-wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.	Rarely (0-50% of the time)																
4.b.	When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).	Rarely (0-50% of the time)																
4.c.	Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly).	Rarely (0-50% of the time)																
4.d.	Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	Rarely (0-50% of the time)																
4.e.	IG findings are incorporated into the POA&M process.	Rarely (0-50% of the time)																
4.f.	POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.	Rarely (0-50% of the time)																
<b>POA&amp;M process comments:</b>																		
<b>Question 5: IG Assessment of the Certification and Accreditation Process</b>																		
<p>Provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Provide narrative comments as appropriate.</p> <p>Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May 2004) for certification and accreditation work initiated after May 2004. This includes use of the FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems" (February 2004) to determine a system impact level, as well as associated NIST document used as guidance for completing risk assessments and security plans.</p>																		
5.a.	<p><b>The IG rates the overall quality of the Agency's certification and accreditation process as:</b></p> <p>Response Categories:</p> <ul style="list-style-type: none"> <li>- Excellent</li> <li>- Good</li> <li>- Satisfactory</li> <li>- Poor</li> <li>- Failing</li> </ul>	Satisfactory																
5.b.	<p><b>The IG's quality rating included or considered the following aspects of the C&amp;A process:</b> (check all that apply)</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 70%;">Security plan</td> <td style="width: 30%; text-align: center;">X</td> </tr> <tr> <td>System impact level</td> <td style="text-align: center;">X</td> </tr> <tr> <td>System test and evaluation</td> <td style="text-align: center;">X</td> </tr> <tr> <td>Security control testing</td> <td style="text-align: center;">X</td> </tr> <tr> <td>Incident handling</td> <td style="text-align: center;">X</td> </tr> <tr> <td>Security awareness training</td> <td></td> </tr> <tr> <td>Configurations/patching</td> <td></td> </tr> <tr> <td>Other:</td> <td>Risk Assessment, Contingency Plan and POAM</td> </tr> </table>	Security plan	X	System impact level	X	System test and evaluation	X	Security control testing	X	Incident handling	X	Security awareness training		Configurations/patching		Other:	Risk Assessment, Contingency Plan and POAM	
Security plan	X																	
System impact level	X																	
System test and evaluation	X																	
Security control testing	X																	
Incident handling	X																	
Security awareness training																		
Configurations/patching																		
Other:	Risk Assessment, Contingency Plan and POAM																	
<b>C&amp;A process comments:</b>																		

Section C - Inspector General: Questions 6, 7, and 8		
<b>Agency Name:</b>	Department of Transportation	
Question 6-7: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process		
6	<p>Provide a qualitative assessment of the agency's Privacy Impact Assessment (PIA) process, as discussed in Section D Question #5 (SAOP reporting template), including adherence to existing policy, guidance, and standards.</p> <p>Response Categories:</p> <ul style="list-style-type: none"> <li>- Response Categories:</li> <li>- Excellent</li> <li>- Good</li> <li>- Satisfactory</li> <li>- Poor</li> <li>- Failing</li> </ul>	Satisfactory
<b>Comments:</b>		
7	<p>Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-07-16 Safeguarding Against and Responding to the Breach of Personally Identifiable Information.</p> <p>Response Categories:</p> <ul style="list-style-type: none"> <li>- Response Categories:</li> <li>- Excellent</li> <li>- Good</li> <li>- Satisfactory</li> <li>- Poor</li> <li>- Failing</li> </ul>	Failing
<b>Comments:</b>	DOT Breach Policy is in Draft and still undergoing revision. This policy should had been issued by September 2007. DOT has not completed its review to determine which IT systems contain PII. Therefore, the Privacy Officer could not provide assurance that the unreviewed IT systems do not contain PII. DOT has not implemented a plan to reduce social security numbers. DOT doe not have rules of behavior and consequences policy in place.	
Question 8: Configuration Management		
8.a.	Is there an agency-wide security configuration policy? Yes or No.	No
<b>Comments:</b>	DOT does not have a security configuration policy in place. This policy is under development.	
8.b.	<p>Approximate the extent to which applicable systems implement common security configurations, including use of common security configurations available from the National Institute of Standards and Technology's website at <a href="http://checklists.nist.gov">http://checklists.nist.gov</a>.</p> <p>Response categories:</p>	Rarely (0-50% of the time)
	<ul style="list-style-type: none"> <li>- Rarely- for example, approximately 0-50% of the time</li> <li>- Sometimes- for example, approximately 51-70% of the time</li> <li>- Frequently- for example, approximately 71-80% of the time</li> <li>- Mostly- for example, approximately 81-95% of the time</li> <li>- Almost Always- for example, approximately 96-100% of the time</li> </ul>	
8.c.	Indicate which aspects of Federal Desktop Core Configuration (FDCC) have been implemented as of this report:	
	c.1. Agency has adopted and implemented FDCC standard configurations and has documented deviations. Yes or No.	No
	c.2 New Federal Acquisition Regulation 2007-004 language, which modified "Part 39—Acquisition of Information Technology", is included in all contracts related to common security settings. Yes or No.	No
	c.3 All Windows XP and VISTA computing systems have implemented the FDCC security settings. Yes or No.	No

Section C - Inspector General: Questions 9, 10 and 11		
<b>Agency Name:</b>	Department of Transportation	
<b>Question 9: Incident Reporting</b>		
Indicate whether or not the agency follows documented policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement. If appropriate or necessary, include comments in the area provided below.		
9.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	No
9.b.	The agency follows documented policies and procedures for external reporting to US-CERT. Yes or No. ( <a href="http://www.us-cert.gov">http://www.us-cert.gov</a> )	Yes
9.c.	The agency follows documented policies and procedures for reporting to law enforcement. Yes or No.	Yes
Comments:	We found that ten incidents involving PII were not reported within the 1-hour requirement; some were many days late. The CIO viewed these as a small subset of a much larger universe of security incidents. However, considering the importance of timely reporting of sensitive breaches concerning privacy information, we concluded that the Department did not follow documented policies and procedures for reporting incidents internally.	
<b>Question 10: Security Awareness Training</b>		
Has the agency ensured security awareness training of all employees, including contractors and those employees with significant IT security responsibilities?		Rarely (0-50% of employees)
Response Categories: - Rarely- or approximately 0-50% of employees - Sometimes- or approximately 51-70% of employees - Frequently- or approximately 71-80% of employees - Mostly- or approximately 81-95% of employees - Almost Always- or approximately 96-100% of employees		
<b>Question 11: Collaborative Web Technologies and Peer-to-Peer File Sharing</b>		
Does the agency explain policies regarding the use of collaborative web technologies and peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training? Yes or No.		No
<b>Question 12: E-Authentication Risk Assessments</b>		
12.a. Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with the NIST Special Publication 800-63, "Electronic Authentication Guidelines"? Yes or No.		No
12.b. If the response is "No", then please identify the systems in which the agency has not implemented the e-authentication guidance and indicate if the agency has a planned date of remediation.		The three systems that OIG reviewed had not implemented e-authentication guidance.

## **EXHIBIT B. SCOPE AND METHODOLOGY**

The Federal Information Security Management Act of 2002 (FISMA) requires that we perform an independent evaluation to determine the effectiveness of the Department's information security program and practices. FISMA further requires that our evaluation include testing of a representative subset of systems and an assessment, based on our testing, of the Department's compliance with FISMA and applicable requirements. On July 14, 2008, the Office of Management and Budget (OMB) issued M-08-21, *Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, which provides instructions for inspectors general for completing their FISMA evaluations and the required OMB template.

To meet FISMA and OMB requirements, we selected a representative subset of 16 departmental systems (see Table 7) and reviewed the compliance of these systems with NIST and OMB requirements in the areas of risk categorization, security plans, annual control testing, contingency planning, certification and accreditation, incident handling, and plans of actions and milestones. We also conducted testing to assess the Department's inventory, its overall process of resolving information security weaknesses, certain privacy requirements, configuration management, incident reporting, security-awareness training, and e-authentication. Our tests included analysis of data contained in the Department's Cyber Security Assessment and Management system, reviews of supporting documentation, and interviews with departmental officials. We also used commercial scanning software to assess network vulnerabilities and compliance with Federal Desktop Core Configuration requirements.

For FY 2008, we determined that work pertaining to Earned Value Management (EVM) would no longer be included within the scope of our FISMA audit and will be included in a separate report. In addition, we determined that audit work and findings developed specific to FAA's business continuity plans and to its testing of operational systems outside of the computer laboratory would be the subject of a separate report. We did, however, include eleven FAA systems in our sample to ensure adequate representation of FAA and considered FAA data as it related to our overall conclusions on DOT's information security program and practices.

**Table 7. OIG's Representative Subset of DOT Systems**

<b>Operating Administration</b>	<b>System</b>	<b>Contractor System?</b>
FAA	Automated Surface Observing System Controller Equipment/Integrated Display System (ACE-IDS)	No
FAA	Automated Weather Observation System Data Acquisition System (ADAS)	No
FAA	CAPSTONE	No
FAA	Automated Radar Terminal System IIIA (ARTS IIIA)	No
FAA	Cyber Security Assessment and Management (CSAM)	No
FAA	FALCON	No
FAA	Human Resources -Grievance Electronic Tracking System (GETS)	No
FAA	Logical Access & Authorization Control (LAACS)	No
FAA	On-Line Aviation Safety Inspection System—Office of Aviation Safety (OASIS-AVS)	No
FAA	Parts Reporting System (PRS)	No
FAA	Weather Messaging Switching Center Replacement Sustainment (WMSCR)	No
FHWA	FHWA Network/LAN/WAN	No
FMCSA	Hazardous Materials Package Inspection Program (HMPIP)	No
FRA	Automated Track Inspection Program (ATIP)	Yes
OST	Data Center Common Operating Environment (COE)	Yes
RITA	Intermodal Transportation Database (ITDB)/TranStats	No

Source: OIG

As required by OMB, we completed the FISMA template, which captured key security metrics and qualitative assessments pertaining to DOT's information security program and practices. We also reviewed the Department's progress in resolving weakness identified in our prior year's FISMA report and compared our current FISMA template to the prior template. OMB requires that the FISMA template include information from all DOT Operating Administrations, including OIG.

## **Exhibit B. Scope and Methodology**

We performed our information security review work throughout FY 2008, focusing on OMB's FISMA template between June 2008 and September 2008. We conducted our work at departmental and Operating Administration Headquarters offices in the Washington, D. C., area. We conducted our audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Previous audit reports on the Department's information security program issued in response to the FISMA legislative mandate (formerly the Government Information Security Reform Act) include:

*DOT Information Security Program*, FI-2008-001, October 10, 2007;  
*DOT Information Security Program*, FI-2007-002, October 23, 2006;  
*DOT Information Security Program*, FI-2006-002, October 7, 2005;  
*DOT Information Security Program*, FI-2005-001, October 1, 2004;  
*DOT Information Security Program*, FI-2003-086, September 25, 2003;  
*DOT Information Security Program*, FI-2002-115, September 27, 2002; and  
*DOT Information Security Program*, FI-2001-090, September 7, 2001.

## EXHIBIT C. DEPARTMENTAL OPERATING ADMINISTRATIONS AND SYSTEM INVENTORY COUNTS

Operating Administration	FY 2008	FY 2007
Federal Aviation Administration (FAA)	264	264
Federal Highway Administration (FHWA)	26	25
Federal Motor Carrier Safety Administration (FMCSA)	23	23
Federal Railroad Administration (FRA)	21	20
Federal Transit Administration (FTA)	5	5
Maritime Administration (MARAD)	13	11
National Highway Traffic Safety Administration (NHTSA)	11	18
Office of Inspector General (OIG)	2	3
Office of the Secretary (OST)	44	42
Pipeline and Hazardous Materials Safety Administration (PHMSA)	4	5
Research and Innovative Technology Administration (RITA)	9	10
Saint Lawrence Seaway Development Corporation (SLSDC)	1	1
Surface Transportation Board (STB)	2	2
<b>Total Systems</b>	<b>425</b>	<b>429</b>

Source: OIG and DOT



## EXHIBIT D. COMPARISON OF FISMA RESULTS FROM FY 2007 TO FY 2008

Template Question No.	OMB-Required Metrics and/or Qualitative Assessments	FY 2007	FY 2008
2a	Percentage of systems certified and accredited	81%	50%
2b	Percentage of systems tested annually	43%	81%
2c	Percentage with tested contingency plans	19%	56%
3a	Agency performs oversight and evaluation of contractor-owned systems.	Always	Rarely
3b	Agency has developed a complete inventory of major information systems.	Always	Always
3c	IG generally agrees with CIO on number of agency-owned information systems.	Yes	Yes
3d	IG generally agrees with CIO on number of contractor-owned information systems.	Yes	Yes
3e	Inventory is maintained and updated annually.	Yes	Yes
4a	The POA&M is an agencywide process incorporating all known IT security weaknesses.	Sometimes	Rarely
4b	When an IT security weakness is identified, program officials develop, implement, and manage POA&Ms.	Sometimes	Rarely
4c	Officials report their progress on security weakness remediation to the CIO at least quarterly.	Always	Rarely
4d	Agency CIO centrally tracks, maintains, and reviews POA&M activities at least quarterly.	Always	Rarely
4e	IG findings incorporated into POA&M process.	Always	Rarely
4f	POA&M process prioritizes IT security weaknesses.	Frequently	Rarely
5a	Quality of the certification and accreditation process	Satisfactory	Satisfactory
6	Quality of the Privacy Impact Assessment	Good	Satisfactory
7	Quality of the agency's progress in implementing OMB's Breach-Notification Requirements.	N/A	Failing
8a	Is there an agencywide security configuration policy?	Yes	No
8b	Extent to which systems implement common security configurations	Rarely	Rarely
8c1	Agency implemented FDCC standard configurations?	N/A	No
8c2	New acquisition regulations are included in all contracts related to common security settings.	N/A	No
8c3	All Windows XP and VISTA systems have implemented FDCC settings.	N/A	No
9a	Agency follows documented procedures for identifying and reporting incidents internally.	Yes	No
9b	Agency follows documented procedures for reporting incidents to US-CERT.	Yes	Yes
9c	Agency follows documented procedures for reporting incidents to law enforcement.	Yes	Yes
10	Agency has ensured that security training is provided to employees and contractors.	Frequently	Rarely
11	Agency explains policies regarding collaborative Web technologies and peer-to-peer file sharing in training.	N/A	No
12	Agency identified and validated all e-authentication applications.	N/A	No

Source: OIG

## EXHIBIT E. STATUS OF PRIOR YEAR'S RECOMMENDATIONS

FY 2007 FISMA Report Recommendation Number	FY 2007 Recommendation	Status
1	Enhance the protection of information systems by working with the Acting FAA Administrator to establish target dates for correcting air traffic control systems' risk categorization in accordance with departmental policy.	To Be Addressed in a Separate Report
2	Enhance the protection of information systems by working with the affected Operating Administrations to ensure proper risk categorization and security protection of systems containing personally identifiable information.	Addressed in a Separate Report
3	Enhance the protection of information systems by requiring Operating Administration CIOs and system owners to identify and implement security upgrades needed to meet minimum security standards by March 31, 2008.	Replaced by FY 2008 Recommendation #27
4	Enhance the protection of information systems by establishing a security test and evaluation process for all departmental systems operating on the common IT infrastructure after the security controls review is complete for the expanded infrastructure.	Open
5	Enhance correction of identified security deficiencies by working with Operating Administrators to develop measures of accountability that would hold Operating Administration CIOs and system owners responsible for timely correction and decisions to support cancellations of identified security weaknesses, such as incorporating these measures as part of their performance standards.	Replaced by FY 2008 Recommendations #20, 21, 22

FY 2007 FISMA Report Recommendation Number	FY 2007 Recommendation	Status
6	Enhance network security configuration by working with Operating Administrations to establish an effective methodology to ensure that commercial software products used in departmental systems are configured in accordance with security standards; and by deploying an automated tool to systematically verify compliance with departmental baseline configuration standards.	Replaced by FY 2008 Recommendations #8, 9, 10
7	Enhance network security configuration by finalizing the secure remote access implementation and management policy; and continuing to explore alternatives to using employee home computers for telework, such as having a pool of Government-issued laptop computers that are properly configured and in compliance with departmental security standards to support telework.	Open
8	Ensure the consistency and timeliness of security-incident reporting by directing the FAA CSIRC to establish consistent procedures to ensure that all security incidents are reported to the Department and US-CERT in a timely manner.	Replaced by FY 2008 Recommendations #12, 13
9	Ensure the consistency and timeliness of security-incident reporting by conducting periodic reviews of the effectiveness of FAA's security-incident-reporting practice	Open
10	Ensure the consistency and timeliness of security-incident reporting by working with the FAA CIO to ensure accurate security performance measurement reporting in the Performance and Accountability Report to OMB and the Congress.	Open

Source: OIG

**Exhibit E. Status of Prior Year's Recommendations**

**EXHIBIT F. MAJOR CONTRIBUTORS TO THIS REPORT**

<b>Name</b>	<b>Title</b>
Rebecca C. Leng	Assistant Inspector General for Financial and Information Technology Audits
Louis C. King	Program Director
Dr. Ping Z. Sun	Program Director for IT Audit Computer Laboratory
James Mallow	Project Manager
Lissette Mercado	Project Manager
Michael P. Fruitman	Communications Adviser
Vasily Gerasimov	Information Technology Specialist
Martha Morrobel	Information Technology Specialist
Anthony Cincotta	Information Technology Specialist

## APPENDIX. MANAGEMENT COMMENTS




U.S. Department of  
Transportation  
Office of the Secretary  
of Transportation

# Memorandum

Subject: Response to OIG Input to FISMA Report (Exhibit A),  
for the Audit of the DOT Information Security Program,  
DOT

Date: October 7, 2008

From:   
Dan Mintz  
DOT Chief Information Officer

Reply to Attn.  
of:

To: Calvin L. Scovel, III  
DOT Inspector General

The Department of Transportation (DOT) Chief Information Officer (CIO) reviewed the Office Of Inspector General (OIG's) draft final FY 2008 Information Security Program Audit Report and provided oral comments.

The CIO concurred with the report's findings and recommendations and will provide written comments describing the specific actions and milestones that will be taken to implement the recommendations, thirty (30) days after the signing date of the official FY 2008 FISMA Report.

Subsequent to its review, the CIO was pleased to note that actions are already being taken in many areas to address the recommendations of the audit team, including:

- The CIO allowed for an additional thirty (30) days of activity by the modes beyond the OIG audit cutoff of August 31, 2008. The additional inputs obtained during that period contribute to differences between the CIO's overall assessment of the Department and findings by the OIG (Exhibit D). As a consequence, the CIO will evaluate and establish a "FISMA year" to avoid these differences during subsequent FISMA evaluation cycles within the first quarter of FY2009.
- In the area of incident response and reporting, the CIO is renewing the memorandum of agreement with the Federal Aviation Administration (FAA) for services provided to the Department by the Cyber Security Management Center (CSMC), expects to have the Secretarial Charter for the CSMC Board signed by the end of Q1 FY2009, and has assigned a resource to review and enhance reporting and metrics, and to provide oversight of modal plans to provide increased network visibility to the CSMC by the end of Q2 FY2009. In establishing the CSMC via Secretarial charter, it is instantiated as a Departmental entity with direct accountability to the Secretary, has durability in that it requires

Secretarial action to revoke the charter, and it serves to elevate situational awareness and incident response to the attention of senior management.

- As required by M-07-16, the DOT CIO and Senior Agency Official for Privacy (SAOP) has established an agency response team for privacy, and the required policy documents for Breach Notification, and Rules and Consequences are in review prior to issuance in Q1 of FY2009. Evaluation of options to protect privacy information on the Departmental network is planned to occur in Q1 FY2009, with a recommendation to the DOT CIO and DOT CIO Council to occur early in Q2 FY2009.
- To strengthen its configuration management policy and implementation across the Department, the CIO has assigned a resource to provide oversight of the DOT FDCC initiative, including an evaluation and rebaseline of the current plan by the end of Q1 FY2009, and will issue updated policy, complete deployment of an automated compliance solution already in progress, and begin regular monthly and quarterly reporting and reviews of modal progress towards compliance by the end of Q1 FY2009.
- To strengthen its POAM management and quarterly compliance review process, a resource has already been assigned to elevate the Department's verification and validation processes for information assurance and privacy, with a goal of improving the effectiveness of compliance reviews beginning the end of Q1 FY2009. As part of the process improvement, monthly reporting and the quarterly compliance reviews will be revised to incorporate escalation of unremediated POAM's or weaknesses to successively higher levels of DOT management with the goal of driving towards successful remediation or explicit acceptance of risk.
- Lastly, as a measure to reinforce accountability of leadership for the information assurance and privacy performance of their organizations, the CIO has already begun efforts to incorporate appropriate performance elements into the performance plans of modal CIO's, and the accountability agreements of modal administrators. As part of that process, the CIO will solicit the input of OIG on the proposed metrics. For FY2009 it is expected that this will occur as a pilot effort, with a CIO objective of institutionalizing the performance elements beginning with the FY2010 evaluation cycle.

The OCIO office appreciates the working relationship developed during this audit and looks forward to the OIG's continued involvement during FY2009 with "Getting back to Green" remediation efforts.

If you have any questions, please feel free to call me on 202-366-9201 or have a member of your staff call Andrew Orndorff on 202-366-7111.

cc: Rebecca Leng, JA-20  
Martin Gertel, M-1

## **Appendix. Management Comments**

The following pages contain textual versions of the graphs and charts found in this document. These pages were not in the original document but have been added here to accommodate assistive technology.

## **Information Security Program Section 508 Compliance Presentation**

### **Table 4. IT Security Weaknesses Overdue for Mitigation**

The Surface Transportation Board (STB) has 67 total IT security weaknesses. Of this total, all 67 are overdue or without a scheduled completion date. Specifically, 52 are more than one year overdue and 15 have no completion date.

The Saint Lawrence Seaway Development Corporation (SLSDC) has no IT security weaknesses.

The Research and Innovative Technology Administration (RITA) has 59 total IT security weaknesses. Of this total, all 59 are overdue or without a scheduled completion date. Specifically, one is 91 to 120 days overdue; six are 121 days to one year overdue; 18 are more than one year overdue and 34 have no completion date.

The Pipeline and Hazardous Materials Safety Administration (PHMSA) has 128 total IT security weaknesses. Of this total, all 128 are overdue or without a scheduled completion date. Specifically, 49 are 61 to 90 days overdue; 24 are 121 days to one year overdue; 27 are more than one year overdue and 28 have no completion date.

The Office of the Secretary of Transportation (OST) has 53 total IT security weaknesses. Of this total, 36 are overdue or without a scheduled completion date. Specifically, one is 61 to 90 days overdue; 14 are 91 to 120 days overdue; three are 121 days to one year overdue; 17 are more than one year overdue and one has no completion date.

The Office of the Inspector General (OIG) has 15 total IT security weaknesses. Of this total, nine are overdue. Specifically, eight are 121 days to one year overdue and one is more than one year overdue.

The National Highway Traffic Safety Administration (NHTSA) has seven total IT security weaknesses. Of this total, six are overdue or without a scheduled completion date. Specifically, four are more than one year overdue and two have no completion date.

The Maritime Administration (MARAD) has 337 total IT security weaknesses. Of this total, five are overdue or without a scheduled completion date. Specifically,



one is one to 60 days overdue; one is 61 to 90 days overdue; one is 91 to 120 days overdue and two have no completion date.

The Federal Transit Administration (FTA) has 17 total IT security weaknesses. Of this total, none are overdue or without a scheduled completion date.

The Federal Rails Administration (FRA) has 257 total IT security weaknesses. Of this total, 181 are overdue or without a scheduled completion date. Specifically, two are one to 60 days overdue; 30 are 91 to 120 days overdue; six are more than one year overdue and 143 have no completion date.

The Federal Motor Carrier Safety Administration (FMCSA) has 28 total IT security weaknesses. Of this total, 9 are overdue. Specifically, three are 61 to 90 days overdue and six are more than one year overdue.

The Federal Aviation Administration (FAA) has 3,049 total IT security weaknesses. Of this total, 217 are overdue or without a scheduled completion date. Specifically, seven are one to 60 days overdue; five are 61 to 90 days overdue; four are 91 to 120 days overdue; two are 121 days to one year overdue; seven are more than one year overdue and 192 have no completion date.

The Federal Highway Administration (FHWA) has 269 total IT security weaknesses. Of this total, all 269 are overdue or without a scheduled completion date. Specifically, two are 91 to 120 days overdue; 31 are 121 days to 1 year overdue; 226 are more than one year overdue and ten have no completion date.

In total, the Department has 4,286 IT security weaknesses. Of this total, 986, or 23 percent, are overdue or without a scheduled completion date. Specifically, ten, or .2 percent, are one to 60 days overdue; 59, or 1.4 percent, are 61 to 90 days overdue; 52, or 1.2 percent, are 91 to 120 days overdue; 74, or 1.7 percent, are 121 days to one year overdue; 364, or 8.5 percent, are more than one year overdue and 427, or ten percent, have no completion date.